10 things you should know about securing wireless connections

Version 1.0
Sept. 22, 2005

By Debra Littlejohn Shinder, MCSE, MVP

Wireless networking is easy to set up, and it's convenient, especially if you like to move around the house or office without your portable computer while staying connected. But because they use the airwaves, wireless communications are more vulnerable to interception and attack than a wired connection. Here are some tips for securing your wireless network.

Table of contents

1 Use encryption

Encryption is the number one security measure, but many wireless access points (WAPs) don't have encryption enabled by default. Although most WAPs support the Wired Equivalent Privacy (WEP) protocol, it's not enabled by default. WEP has a number of security flaws, and a knowledgeable hacker can crack it, but it's better than no encryption at all. Be sure to set the WEP authentication method for "shared key" rather than "open system." The latter does *not* encrypt the data; it only authenticates the client. Change the WEP key frequently and use 128-bit WEP rather than 40 bit.

2 Use *strong* encryption

Because of WEP's weaknesses, you should use the Wi-Fi Protected Access (WPA) protocol instead of WEP if possible. To use WPA, your WAP must support it (you may be able to add support to an older WAP with a firmware upgrade);your wireless network access cards (NICs) must support it (again, a firmware update may be necessary); and your wireless client software must support it. Windows XP Service Pack 2 installs the WPA client. SP1 machines can be updated to support WPA by installing the Windows WPA client with the Wireless Update Rollup Package (see http://support.microsoft.com/kb/826942/). Another encryption option is to use IPsec, if your wireless router supports it.

3 Change the default administrative password

Most manufacturers use the same default administrative password for all their wireless access points (or at least, all those of a particular model). Those default passwords are common knowledge among hackers, who can use them to change your WAP settings. The first thing you should do when you set up a WAP is change the default password to a strong password (eight characters or more in length, using a combination of alpha and numeric characters, not using words that are in the dictionary).

4 Turn off SSID broadcasting

The Service Set Identifier (SSID) is the name of your wireless network. By default, most WAPs broadcast the SSID. This makes it easy for users to find the network, as it shows up on their list of available networks on their wireless client computers. If you turn off broadcasting, users will have to know the SSID to connect. Some folks will tell you that turning off SSID broadcasting is useless because a hacker can use packet sniffing software to capture the SSID even if broadcasting is turned off. That's true, but why make it easier for them? That's like saying burglars can buy lockpicks, so locking the door is useless. Turning off broadcasting won't deter a serious hacker, but it will protect from the casual "piggybacker" (for example, a next door neighbor who notices the new network and decides to try connecting "just for fun").

5 Turn off the WAP when not in use

This one may seem simplistic, but few companies or individuals do it. If you have wireless users connecting only at certain times, there's no reason to run the wireless network all the time and provide an opportunity for intruders. You can turn off the access point when it's not in use—such as at night when everyone goes home and there is no need for anyone to connect wirelessly.

6 Change the default SSID

Manufacturers provide a default SSID, often the equipment name (such as Linksys). The purpose of turning off SSID broadcasting was to prevent others from knowing the network name, but if you use the default name, it's not too difficult to guess. As mentioned, hackers can use tools to sniff the SSID, so don't change the name to something that gives them information about you or your company (such as the company name or your physical address).

7 Use MAC filtering

Most WAPs (although not some of the cheapest ones) will allow you to use media access control (MAC) address filtering. This means you can set up a sort of “white list” of computers that are allowed to connect to your wireless network, based on the MAC or physical addresses assigned to their network cards. Communications from MAC addresses that aren’t on the list will be refused.

The method isn’t foolproof, since it’s possible for hackers to capture packets transmitted over the wireless network and determine a valid MAC address of one of your users and then spoof the address. But it does make things more difficult for a would-be intruder, and that’s what security is really all about.

8 Isolate the wireless network from the rest of the LAN

To protect your wired internal network from threats coming over the wireless network, create a wireless DMZ or perimeter network that’s isolated from the LAN. That means placing a firewall between the wireless network and the LAN. Then you can require that in order for any wireless client to access resources on the internal network, he or she will have to authenticate with a remote access server and/or use a VPN. This provides an extra layer of protection.

For instructions on how to allow VPN access to your network from a wireless DMZ created with Microsoft’s ISA Server firewall, see http://techrepublic.com.com/5100-6350_11-5807148.html. [You'll need a TechProGuild subscription to access this content.]

9 Control the wireless signal

The typical 802.11b WAP transmits up to about 300 feet. However, this range can be extended by a more sensitive antenna. By attaching a high gain external antenna to your WAP, you can get a longer reach but this may expose you to war drivers and others outside your building. A directional antenna will transmit the signal in a particular direction, instead of in a circle like the omnidirectional antenna that usually comes built into the WAP. Thus, through antenna selection you can control both the signal range and its direction to help protect from outsiders. In addition, some WAPs allow you to adjust signal strength and direction via their settings.

10 Transmit on a different frequency

One way to “hide” from hackers who use the more common 802.11b/g wireless technology is to go with 802.11a instead. Since it operates on a different frequency (the 5 GHz range, as opposed to the 2.4 GHz range in which b/g operate), NICs made for the more common wireless technologies won’t pick up its signals. Sure, this is a type of “security through obscurity”—but it’s perfectly valid when used in conjunction with other security measures. After all, security through obscurity is exactly what we advocate when we tell people not to let others know their social security numbers and other identification information.

A drawback of 802.11a, and one of the reasons it’s less popular than b/g, is that the range is shorter: about half the distance of b/g. It also has difficulty penetrating walls and obstacles. From a security standpoint, this “disadvantage” is actually an advantage, as it makes it more difficult for an outsider to intercept the signal even with equipment designed for the technology.

Debra Littlejohn Shinder is a technology consultant, trainer and writer who has authored a number of books on computer operating systems, networking, and security. These include *Scene of the Cybercrime: Computer Forensics Handbook*, published by Syngress, and *Computer Networking Essentials*, published by Cisco Press. She is co-author, with her husband, Dr. Thomas Shinder, of *Troubleshooting Windows 2000 TCP/IP*, the best-selling *Configuring ISA Server 2000*, and *ISA Server and Beyond*.

Additional resources

- TechRepublic's **Downloads RSS Feed** XML
- Sign up for our Downloads Weekly Update newsletter
- Sign up for our Network Security NetNote
- Check out all of TechRepublic's free newsletters
- "Strengthen your wireless security by avoiding these missteps" (TechRepublic download)
- "Lock IT Down: How to conduct a wireless security audit" (TechRepublic article)
- "Secure your enterprise wireless network with this Cisco Press sample chapter" (TechRepublic download)
- "Wireless security" (TechRepublic download)

Version history

Version: 1.0
Published: September 22, 2005

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to drop us a line and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team